(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平10－171909

(43)公開日　平成10年(1998)６月26日

(51)Int.Cl.[6]		識別記号	ＦＩ		
Ｇ０６Ｆ	19/00		Ｇ０６Ｆ	15/30	３５０
	15/00	３３０		15/00	３３０Ｅ
	17/60		Ｇ０９Ｃ	1/00	６６０Ａ
Ｇ０９Ｃ	1/00	６６０	Ｇ０６Ｆ	15/21	３４０Ｂ
Ｈ０４Ｌ	9/32			15/30	３４０

審査請求　未請求　請求項の数12　ＯＬ　（全 14 頁）　最終頁に続く

(21)出願番号　特願平9－271437

(22)出願日　平成９年(1997)10月３日

(31)優先権主張番号　１９９６－４４１２５

(32)優先日　1996年10月５日

(33)優先権主張国　韓国（ＫＲ）

(71)出願人　390019839
三星電子株式会社
大韓民国京畿道水原市八達区梅灘洞416

(72)発明者　柳　周　烈
大韓民国ソウル特別市松坡区風納２洞508番地漢江極東アパート104棟1601号

(72)発明者　鄭　鎬　碩
大韓民国漢城市瑞草区方背１洞914－12番地松岩ヴィラ301号

(72)発明者　文　スーン　一
大韓民国漢城市瑞草区瑞草３洞1468－１番地三星生活館ビー棟302号

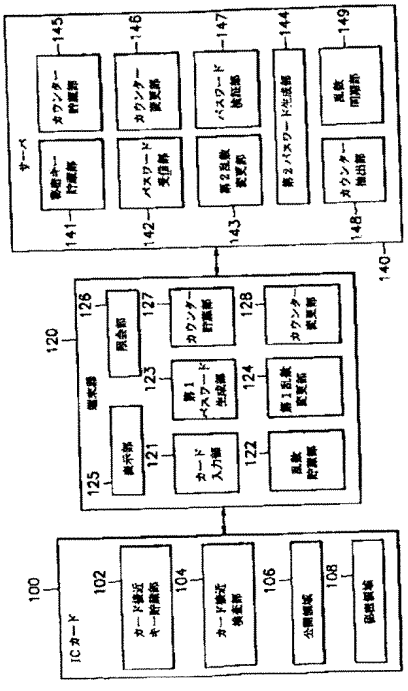
(74)代理人　弁理士　三好　秀和　（外１名）

(54)【発明の名称】　使用者認証装置及びその方法

(57)【要約】

【課題】　電子貨幣の残額及び取引照会機能と一回用のパスワード発生機能を有する携帯用端末器とICカードを用いた使用者認証装置及びその方法を提供する。

【解決手段】　本発明の使用者認証装置は、秘密キー等を貯蔵するICカード１００と、ICカードを受取るカード入力部１２１と、乱数を読出して貯蔵する乱数貯蔵部１２２と、一回用のパスワードを生成する第1パスワード生成部１２３と、乱数値を変更する第1乱数変更部１２４と、処理結果を表示する表示部１２５とを具備する端末器１２０と、秘密キー等を貯蔵する秘密キー貯蔵部１４１と、一回用のパスワードを生成する第2パスワード生成部１４４と、乱数値を貯蔵する第2乱数変更部１４３と、一回用のパスワードを受信するパスワード受信部１４２と、パスワードを検証するパスワード検証部１４７とを具備するサーバ１４０とを含むことを特徴とする。



1

【特許請求の範囲】

【請求項１】　一回用のパスワードを生成するための秘密キー及び所定の乱数を貯蔵しているICカードと、このICカードを入力として一回用のパスワードを生成する端末器と、この端末器から生成された一回用のパスワードを認証するサーバとを含む使用者認証装置であって、

前記端末器は、

前記ICカードを受取るインタフェースを行い、前記ICカードが最初に入力されたカードであるか否かを判別するカード入力部と、

前記ICカードが最初に前記カード入力部に挿入されたときには前記ICカードの乱数を読出して貯蔵し、前記ICカードの乱数を削除する乱数貯蔵部と、

前記ICカードの秘密キーと前記乱数貯蔵部に貯蔵された乱数を読出して所定の方法により一回用のパスワードを生成する第1パスワード生成部と、

前記第1パスワード生成部から一回用のパスワードが生成されると前記乱数貯蔵部に貯蔵された乱数値を所定の値に変更させて前記乱数貯蔵部に貯蔵させる第1乱数変更部と、

前記端末器及びサーバの処理結果をディスプレーする表示部を少なくとも具備し、

前記サーバは、

前記ICカードに最初に貯蔵された秘密キー及び所定の乱数と同一な秘密キー及び乱数を貯蔵する秘密キー貯蔵部と、

前記秘密キー貯蔵部に貯蔵された秘密キーと乱数を読出して前記端末器における所定の方法と同一な方法により一回用のパスワードを生成する第2パスワード生成部と、

前記第2パスワード生成部から一回用のパスワードが生成されると前記秘密キー貯蔵部の乱数値を前記端末器の乱数変更部と同一に乱数値を変更し、前記秘密キー貯蔵部に貯蔵する第2乱数変更部と、

前記端末器から生成された一回用のパスワードを電話線や所定のネットワークを通して受信するパスワード受信部と、

前記受信されたパスワードと前記生成されたパスワードとが同一なのかを検証するパスワード検証部とを少なくとも具備し、使用者が正当な使用者なのかを認証することを特徴とする使用者認証装置。

【請求項２】　前記ICカードは身分証や電子貨幣兼用であり、使用者の身分認証のための秘密値を安全に貯蔵していることを特徴とする請求項１に記載の使用者認証装置。

【請求項３】　前記端末器の秘密キーは使用者登録過程においてサービス提供者が前記端末器に挿入することを特徴とする請求項１に記載の使用者認証装置。

【請求項４】　前記ICカードは、

無条件に接近しうる公開領域及び外部の接近を許すためにはカード接近キーを要求する秘密領域を具備し、前記秘密領域の接近に必要なカード接近キーを安全に貯蔵するカード接近キー貯蔵部と、

前記外部から入力されるカード接近キーと前記カード接近キー貯蔵部に貯蔵されているカード接近キーとを比べて内部情報の接近の許否を決定するカード接近検査部をさらに具備し、

前記端末器の乱数貯蔵部は、

前記ICカードが最初に前記カード入力部に挿入されると前記ICカードの乱数及びカード接近キーを読出して貯蔵し、前記ICカードの公開領域に貯蔵された乱数とカード接近キーとを削除する乱数貯蔵部であることを特徴とする請求項１に記載の使用者認証装置。

【請求項５】　前記端末器は前記ICカードの残額及び取引内訳を照会する照会部をさらに具備することを特徴とする請求項１に記載の使用者認証装置。

【請求項６】　前記端末器の第1パスワード生成部は、

前記ICカードの秘密キーと前記乱数貯蔵部の乱数を読出して前記秘密キー及び乱数を対称キー暗号アルゴリズムを使用して暗号を生成する対称キー暗号部と、

前記対称キー暗号部から生成された暗号を一方向ハッシュ関数により変換させて前記秘密キーの逆追跡を防止するハッシュ関数部と、

前記ハッシュ関数部から出力される暗号を使用者が読みやすく所定のフォーマットに変換するフォーマット変換部とを含み、前記サーバの第2パスワード生成部は、

前記秘密キー貯蔵部に貯蔵された秘密キー及び乱数を読出して前記秘密キー及び乱数を対称キー暗号アルゴリズムを使用して暗号を生成する対称キー暗号部と、

前記対称キー暗号部から生成された暗号を一方向ハッシュ関数により逆追跡を防止するハッシュ関数遂行部と、

前記ハッシュ関数遂行部から出力される暗号を所定のフォーマットに変換するフォーマット変換部とからなることを特徴とする請求項１または４に記載の使用者認証装置。

【請求項７】　前記端末器及びサーバは、

端末器とサーバの同期を合せるためのカウンター値を貯蔵するカウンター貯蔵部と、

一回用のパスワードを一回生成する度に前記カウンター値を所定の値に変更させて前記カウンター貯蔵部に貯蔵させるカウンター変更部とをさらに具備し、

前記第1パスワード生成部のフォーマット変換部及び第2パスワード生成部のフォーマット変換部は、

前記ハッシュ関数遂行部から出力されるパスワードビット列に前記カウンター貯蔵部のカウンター値を挿入するカウンター挿入部をさらに具備し、

前記サーバは、

前記パスワード受信部により受信された一回用のパスワードからカウンター値を抽出するカウンター抽出部と、

前記カウンター抽出部から抽出されたカウンター値と前

記サーバのカウンター値とが一致しない場合、前記抽出されたカウンター値に相応する乱数を生成して前記サーバの対称キー暗号部に入力させる乱数同期部とをさらに具備することを特徴とする請求項６に記載の使用者認証装置。

【請求項８】　前記フォーマット変換部は2進数の数を10進数に変換することを特徴とする請求項６または７に記載の使用者認証装置。

【請求項９】　前記端末器及びサーバのカウンター挿入部は、

少なくとも１つ以上の一回用のパスワード生成アルゴリズムのプロトコルを示すPTSビットを追加挿入し、前記サーバのカウンター抽出部は、前記PTSビットをさらに抽出し、前記端末器及びサーバの第1、第2パスワード生成部は、前記PTSの情報に応じる一回用のパスワード生成アルゴリズムにより一回用のパスワードを生成するパスワード生成部であることを特徴とする請求項７に記載の使用者認証装置。

【請求項１０】　一回用のパスワードを生成するための秘密キーを貯蔵し、所定の乱数を有しているICカードと、前記ICカードを入力として一回用のパスワードを生成する端末器と、前記ICカードと同一な秘密キーと乱数とを貯蔵しており、前記端末器から生成された一回用のパスワードを認証するサーバとを含む使用者認証装置における使用者認証方法であって、

前記ICカードを前記端末器に挿入する段階と、

前記ICカードが前記端末器に最初に入力されたのかを判断する最初入力判断段階と、

前記最初入力判断段階において最初入力のときには所定のサービス初期化を行ってから一回用のパスワードを生成し、最初入力でないときには一回用のパスワードを生成するパスワード生成段階と、

前記端末器から生成された一回用のパスワードを所定の通信媒体を通して受信し、前記一回用のパスワードを検証する段階とを含むことを特徴とし、

前記パスワード生成段階のサービス初期化は、

前記ICカードの乱数を読出して端末器に貯蔵する段階と、

前記ICカードに貯蔵された乱数を削除する段階よりなり、

前記パスワード生成段階の一回用のパスワード生成は、

前記ICカードの秘密キー及び前記端末器に貯蔵された乱数を読出す第1段階と、

前記秘密キー及び乱数を入力として対称キー暗号アルゴリズムを行う第2段階と、

前記対称キー暗号アルゴリズムを通して出力された値を入力として一方向ハッシュ関数を行う第3段階と、

前記乱数を所定の値に変更して端末器に貯蔵する第4段階と、

前記一方向ハッシュ関数を行って出力された値を所定の

桁数に変換する第5段階とを含んで成され、

前記検証する段階は、

前記端末器から生成された一回用のパスワードを所定の通信媒体を通して受信する受信段階と、

前記サーバに貯蔵している秘密キーと乱数を読出す読出段階と、

前記秘密キー及び乱数を入力として対称キー暗号アルゴリズムを行う段階と、

前記対称キー暗号アルゴリズムを通して出力された値を入力として一方向ハッシュ関数を行う段階と、

前記乱数を所定の値に変更して端末器に貯蔵する値変更段階と、

前記一方向ハッシュ関数を行って出力された値を所定のフォーマットに変換する変換段階と、

前記所定のフォーマットに変換された値と前記受信された一回用のパスワードを比較して同一なら使用者認証をし、異なると使用者認証をしない認証段階を含んでいることを特徴とする使用者認証方法。

【請求項１１】　前記ICカードが秘密領域への接近に必要なカード接近キーをさらに具備するときに、

前記パスワード生成段階のサービス初期化は、

前記ICカードの公開領域から乱数及び秘密領域に接近するためのカード接近キーを読出して端末器に貯蔵する段階と、

前記ICカードの公開領域に貯蔵された乱数及び前記公開領域のカード接近キーを削除する段階よりなり、

前記パスワード生成段階のICカード秘密キー読出は、

前記端末器に貯蔵されたカード接近キーを前記ICカードに入力させる段階と、

前記ICカードに入力されたカード接近キーと前記ICカード秘密領域のカード接近キーが同一ならカード接近を許すカード接近検査段階と、

前記カード接近検査段階で接近が許容されると前記ICカード秘密キーを読出す段階よりなることを特徴とする請求項１０に記載の使用者認証方法。

【請求項１２】　前記端末器及びサーバが端末器とサーバの同期を合せるためのカウンターをさらに具備するときに、

前記パスワード生成段階の一回用のパスワード生成の第4段階は、

前記乱数及びカウンター値を所定の値に変更して端末器に貯蔵する段階であり、

前記パスワード生成段階の一回用のパスワード生成の第5段階は、

前記第3段階から出力されるパスワードビット列に前記カウンター値を挿入する段階と、

前記カウンター値が挿入されたパスワード値を所定のフォーマットに変換する段階よりなり、

前記検証段階の受信段階は、

受信された一回用のパスワードからカウンター値を抽出

する抽出段階と、
前記抽出段階から抽出されたカウンター値と前記サーバのカウンター値とを比較する段階と、
前記比較段階においてカウンター値が一致しない場合、前記カウンターのカウンター値を同一にし、前記乱数値を前記カウンター値に相応する乱数値に変更する段階をさらに具備し、
前記検証段階の値変更段階は、
前記乱数を所定の値に変更して端末器に貯蔵する値変更段階であり、
前記検証段階の変換段階は、
前記一方向ハッシュ関数を行って出力されるパスワードビット列に前記カウンター値を挿入する段階と、
前記カウンター値が挿入されたパスワード値を所定のフォーマットに変換する段階よりなることを特徴とする請求項１０または１１に記載の使用者認証方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は使用者認証システムに係り、特に電子貨幣の残額及び取引照会機能と一回用のパスワード発生機能を有する携帯用端末器と集積回路(IC)カードを用いた使用者認証装置及びその方法に関する。

【０００２】

【従来の技術】コンピュータと通信の発展、広範な電算網の普及と共にメモリと演算機能を有する集積回路(Integrated Circuit：以下ICと称する）カード技術の発展により多様な応用分野が発生して人々には多くの便利さが提供されている。ICカードの応用分野の一種の電子貨幣は電子財布内の残額、取引内訳などを照会する機能が必要である。

【０００３】また、使用者は銀行に直接行かなくても自分の口座にあるお金を管理でき、自宅でコンピュータを用いた遠距離接続により自分の希望する多くの仕事を容易に行うことができる。この際、サービス提供者(銀行、ネットワークサーバ等）はサービスを希望する使用者が正当な権限がある使用者なのかを確認することが必須である。もし、使用者認証システムの性能が低いことによって正当な使用者を仮装した攻撃が成功すると個人の私生活侵害は勿論精神的、物質的に深刻な被害をだすことになる。特に、使用者が遠距離からサービスを希望する場合にサービス提供者は使用者と直接会わない状況で使用者の身分をはっきりと確認できる方法が必要である。

【０００４】使用者の身分を認証するためにはその使用者のみ知っているものやその使用者のみ有しているもの、またはその使用者のみの身体的特徴や習慣などを利用する。今まで使用者の身分を認証するために使われている最も基本的で一般的な方法はパスワード(password)を利用することである。パスワード方式では、その使用者のみが知っているパスワードを確認することにより使用者の身分を認証する。即ち、サービスを受けようとする使用者は最初に自分のみが知っているパスワードを選択してサービス提供者(サーバ)に登録する。使用者は通常数桁の数字や文字をパスワードとして使用する。身分認証を受けることを希望する使用者は自分が覚えているパスワードをサーバに伝達し、サーバはサービス初期に登録された使用者のパスワードと比較して使用者を認証することになる。

【０００５】そして、さらに安全な使用者認証のためには使用者が身分認証を受けようとする度にパスワードが変わる一回用のパスワードを使用することである。これは使用者が認証を受けようとする度にパスワードが変わるので攻撃者が一度パスワードを知ったとしても、これを次回は再び使用することは出来ない。一回用のパスワードを使用して身分認証をするためには使用者が一回用のパスワードを生成できる装置をもつことが必要である。この際、各使用者毎に有している一回用のパスワード生成用の端末器を使用すると、使用者認証のためにその使用者のみが知っていることと、その使用者のみが有しているものを同時に確認するので保安水準を相当高めることができる。

【０００６】一回用のパスワードは既存のパスワードとは異なって毎回他のパスワードを生成するために毎回変わる変数が必要であり、このために時刻(RTC、Real Time Clock)を利用する方法と乱数を利用する方法とがある。

【０００７】時刻を変数として使用する使用者認証方法では、使用者が有する端末器とサービス提供者のサーバとが一致した時間を使用する。即ち、使用者が認証を受けようとする時間に端末器内の時間による一回用のパスワードが発生し、サーバも同時にパスワードを発生させてこの値を比較して使用者認証を行うことになる。

【０００８】また、乱数を用いた方法では、一回用のパスワードを発生させるために乱数発生器を利用して作った乱数値を利用することになる。使用者認証を開始すると、まずサーバが乱数値を生成して使用者に伝達する。端末器はサーバと共有している秘密値でこの乱数値を暗号化して一回用のパスワードを生成し、サーバに伝送する。サーバは端末器と共有している秘密値と自分が伝送した乱数値を使用してパスワードを発生させ、端末器が発生させたパスワードと比較して使用者を認証することになる。

【０００９】

【発明が解決しようとする課題】しかしながら、現在最も広く使われている使用者認証方法であるパスワードを用いた使用者認証方法は多くの問題点を有している。パスワードは通常数桁の数字や文字、例えば個人の情報(電話番号、誕生日、住民登録番号等)を使用するため他人が類推して解かりやすい。使用者は自分が選択したパ

スワードを忘れないようにパスワードをどこかに記録することになるが、これを通して他人に知られる。また、遠距離からサービスを受けようとする使用者が使用者認証を受けるために自分のパスワードを電話線や電算網を通して伝達する場合には盗聴を通して知られやすい。

【００１０】そして、時刻(RTC、Real Time Clock)を用いた使用者認証方法は一回用のパスワードの生成と使用者認証のために使用者の有する端末器とサービス提供者のサーバの時間を正確に一致させなければならない。もし、時間が経過しながら同期が合わないと端末器から生成された一回用のパスワードがサーバから生成されたパスワードと一致しないために正当な使用者に対しても使用者認証に失敗することになる。このように端末器とサーバの同期を合せるためには特別な装置が必要である。従って、既存の応用サービスにおいて使用者認証を強化するために一回用のパスワードを使用するには端末器とサーバの時間を一致させるための特別なサーバが必要なのでサービス提供者には大きな経済的負担となる。また時刻を利用して一回用のパスワードを生成する端末器は使用する変数が時刻であるために、１つの端末器としては唯一つの応用サービスのための一回用のパスワード生成器でのみ使用しうる。使用者が多様な応用サービスを希望する場合には各応用サービス毎にそれぞれの端末器が必要になるという短所がある。

【００１１】乱数を利用する方法は一回用のパスワードを生成するためにサーバが伝送した乱数を端末器に入力しなければならない。これは端末器が入力装置を必ず揃えなければならないという負担がある。また、サーバが先に乱数値を使用者に伝送し、使用者はこの乱数を端末器に入力する過程が必要なので時間が多くかかって使用者には不便である。また、サーバが生成した乱数値を使用者側に伝達できない場合にはこの方法は使用できない。

【００１２】本発明は前述した問題点を解決するために案出されたものであって、その目的は、安くて安全な使用者認証を行うために、電子貨幣の残額と取引内訳を照会しうる機能があり、一回用のパスワード発生機能を同時に収容する携帯用端末器とICカードを用いた使用者認証装置及びその方法を提供することにある。

【００１３】

【課題を解決するための手段】前記目的を達成するための使用者認証装置は、一回用のパスワードを生成するための秘密キー及び所定の乱数を貯蔵しているICカードと、前記ICカードを入力として一回用のパスワードを生成する端末器と、前記端末器から生成された一回用のパスワードを認証するサーバとを含むことが望ましい。前記端末器は、前記ICカードを受取るインタフェースを行い、前記ICカードが最初に入力されたカードであるか否かを判別するカード入力部と、前記ICカードが最初に前記カード入力部に挿入されると前記ICカードの乱数を読出して貯蔵し、前記ICカードの乱数を削除する乱数貯蔵部と、前記ICカードの秘密キーと前記乱数貯蔵部に貯蔵された乱数を読出して所定の方法により一回用のパスワードを生成する第1パスワード生成部と、前記第1パスワード生成部から一回用のパスワードが生成されると前記乱数貯蔵部に貯蔵された乱数値を所定の値に変更して前記乱数貯蔵部に貯蔵する第1乱数変更部と、前記端末器及びサーバの処理結果をディスプレーする表示部を少なくとも具備する。

【００１４】前記サーバは前記ICカードに最初に貯蔵された秘密キー及び所定の乱数と同一な秘密キー及び乱数を貯蔵する秘密キー貯蔵部と、前記秘密キー貯蔵部に貯蔵された秘密キーと乱数を読出して端末器における所定の方法と同一な方法により一回用のパスワードを生成する第2パスワード生成部と、前記第2パスワード生成部から一回用のパスワードが生成されると前記秘密キー貯蔵部の乱数値を前記端末器の乱数変更部と同一に乱数値を変更させ、前記秘密キー貯蔵部に貯蔵させる第2乱数変更部と、前記端末器から生成された一回用のパスワードを電話線や所定のネットワークを通して受信するパスワード受信部と、前記受信されたパスワードと前記生成されたパスワードとが同一であるか否かを検証するパスワード検証部を少なくとも具備する。

【００１５】そして、前記ICカードは外部の接近を許容する公開領域及び外部の接近を制限する秘密領域を具備し、前記秘密領域の接近に必要なカード接近キーを貯蔵するカード接近キー貯蔵部と、前記外部から入力されるカード接近キーと前記カード接近キー貯蔵部に貯蔵されているカード接近キーを比べて内部情報の接近の許否を決定するカード接近検査部をさらに具備する。前記端末器の乱数貯蔵部は前記ICカードが最初に前記カード入力部に挿入されると前記ICカードの乱数及びカード接近キーを読出して貯蔵し、前記ICカードの公開領域に貯蔵された乱数及びカード接近キーを削除する乱数貯蔵部であることが望ましい。

【００１６】また、前記端末器の第1パスワード生成部は前記ICカードの秘密キーと前記乱数貯蔵部の乱数を読出して前記秘密キー及び乱数を対称キー暗号アルゴリズムを使用して暗号を生成する対称キー暗号部と、前記対称キー暗号部から生成された暗号を一方向ハッシュ関数により変換させて前記秘密キーの逆追跡を防止するハッシュ関数部と、前記ハッシュ関数部から出力される暗号を使用者が読みやすく所定のフォーマットに変換するフォーマット変換部とを含む。前記サーバの第2パスワード生成部は前記秘密キー貯蔵部に貯蔵された秘密キー及び乱数を読出して前記秘密キー及び乱数を対称キー暗号アルゴリズムを使用して暗号を生成する対称キー暗号部と、前記対称キー暗号部から生成された暗号を一方向ハッシュ関数により逆追跡を防止するハッシュ関数遂行部と、前記ハッシュ関数遂行部から出力される暗号を所定

のフォーマットに変換するフォーマット変換部よりなることが望ましい。

【００１７】一方、前記目的を達成するための、一回用のパスワードを生成するための秘密キーを貯蔵し、所定の乱数を有しているICカードと、前記ICカードを入力として一回用のパスワードを生成する端末器と、前記ICカードと同一な秘密キーと乱数とを貯蔵しており、前記端末器から生成された一回用のパスワードを認証するサーバとを含む使用者認証装置における使用者認証方法は、前記ICカードを前記端末器に挿入する段階と、前記ICカードが前記端末器に最初に入力されたのかを判断する最初入力判断段階と、前記最初入力判断段階において最初入力なら所定のサービス初期化を行ってから一回用のパスワードを生成し、最初入力でないときには一回用のパスワードを生成するパスワード生成段階と、前記端末器から生成された一回用のパスワードを所定の通信媒体を通して受信し、前記一回用のパスワードを検証する段階とを含むことが望ましい。

【００１８】前記パスワード生成段階のサービス初期化は前記ICカードの乱数を読出して端末器に貯蔵する段階と、前記ICカードに貯蔵された乱数を削除する段階よりなる。

【００１９】前記パスワード生成段階の一回用のパスワード生成は前記ICカードの秘密キー及び前記端末器に貯蔵された乱数を読出す第1段階と、前記秘密キー及び乱数を入力として対称キー暗号アルゴリズムを行う第2段階と、前記対称キー暗号アルゴリズムを通して出力された値を入力として一方向ハッシュ関数を行う第3段階と、前記乱数を所定の値に変更して端末器に貯蔵する第4段階と、前記一方向ハッシュ関数を行って出力された値を所定の桁数に変換する第5段階とを含んで成される。

【００２０】前記検証段階は前記端末器から生成された一回用のパスワードを所定の通信媒体を通して受信する受信段階と、前記サーバに貯蔵している秘密キーと乱数を読出す読出段階と、前記秘密キー及び乱数を入力として対称キー暗号アルゴリズムを行う段階と、前記対称キー暗号アルゴリズムを通して出力された値を入力として一方向ハッシュ関数を行う段階と、前記乱数を所定の値に変更して端末器に貯蔵する値変更段階と、前記一方向ハッシュ関数を行って出力された値を所定のフォーマットに変換する変換段階と、前記所定のフォーマットに変換された値と前記受信された一回用のパスワードを比較して同一なら使用者認証をし、異なるときには使用者認証をしない認証段階とを含んでなされる。

【００２１】そして、前記ICカードがメモリの秘密領域及び公開領域で構成され、前記IC秘密領域への接近に必要なカード接近キーをさらに具備するときには、前記パスワード生成段階のサービス初期化は前記ICカードの公開領域から乱数及び秘密領域に接近するためのカード接近キーを読出して端末器に貯蔵する段階と、前記ICカードの公開領域に貯蔵された乱数及び前記公開領域のカード接近キーを削除する段階よりなり、前記パスワード生成段階のICカード秘密キー読出は前記端末器に貯蔵されたカード接近キーを前記ICカードに入力させる段階と、前記ICカードに入力されたカード接近キーと前記ICカード秘密領域のカード接近キーが同一ならカード接近を許すカード接近検査段階と、前記カード接近検査段階で接近が許容されると前記ICカード秘密キーを読出す段階よりなることが望ましい。

【００２２】また、前記端末器及びサーバが端末器とサーバの同期を合せるためのカウンターをさらに具備するときには、前記パスワード生成段階の一回用のパスワード生成の第4段階は前記乱数及びカウンター値を所定の値に変更して端末器に貯蔵する段階であり、前記パスワード生成段階の一回用のパスワード生成の第5段階は前記第3段階から出力されるパスワードビット列に前記カウンター値を挿入する段階と、前記カウンター値が挿入されたパスワード値を所定のフォーマットに変換する段階よりなり、前記検証段階の受信段階は受信された一回用のパスワードからカウンター値を抽出する抽出段階と、前記抽出段階から抽出されたカウンター値と前記サーバのカウンター値とを比較する段階と、前記比較段階においてカウンター値が一致しない場合、前記カウンターのカウンター値を同一にし、前記乱数値を前記カウンター値に相応する乱数値に変更する段階をさらに具備する。

【００２３】前記検証段階の値変更段階は前記乱数を所定の値に変更して端末器に貯蔵する値変更段階であり、前記検証段階の変換段階は前記一方向ハッシュ関数を行って出力されるパスワードビット列に前記カウンター値を挿入する段階と、前記カウンター値が挿入されたパスワード値を所定のフォーマットに変換する段階よりなることが望ましい。

【００２４】

【発明の実施の形態】以下、添付された図面に基づき本発明の一実施形態を詳しく説明する。

【００２５】図1は本実施形態による使用者認証装置の構成を示したブロック図であって、個人の秘密情報を安全に保管して携帯できる装置のICカード100、携帯しやすく超小型で個人の身分を確認するための一回用のパスワードを生成するだけでなく、電子貨幣の残額を照会しうる複合機能を揃えた端末器120及びこの端末器120で生成された一回用のパスワードを認証して応用サービスを提供するサーバ140により構成されている。

【００２６】ICカード100は一回用のパスワードを生成するための秘密キー及び所定の乱数を貯蔵している所であって、外部の接近を許す公開領域106及び外部の接近を許すためにカード接近キーを要求する秘密領域108を具備し、秘密領域108の接近に必要なカード接近キーを

貯蔵するカード接近キー貯蔵部102及び外部から入力されるカード接近キーと秘密領域に設定されているカード接近キーとを比較して内部情報の接近の可否を決定するカード接近検査部104により構成されている。

【００２７】そして、ICカード100は身分証や電子貨幣としても使用でき、ICカード100の記憶容量は既存のマグネチック(magnetic)カードに比べてかなり大容量であるために使用者が記憶できない多くの情報を保管することができる。また、ICカード内の記憶装置のデータを読出すためにはICカード100のカード接近キーを知っていなければならないので使用者がICカードをなくしても他人が個人の情報を分かりにくい。

【００２８】端末器120はICカード100を受取って一回用のパスワードを生成するブロックであって、カード入力部121、乱数貯蔵部122、第1パスワード生成部123、第1乱数変更部124、表示部125、照会部126、カウンター貯蔵部127及びカウンター変更部128により構成されている。

【００２９】カード入力部121はICカード100を受入れる挿入口を具備し、ICカード100とのインタフェース(interface)機能を行う。乱数貯蔵部122はICカード100が最初にカード入力部121に挿入されるとICカード100に貯蔵されている乱数を読出して、その乱数を貯蔵した後、ICカードに貯蔵されている乱数を削除する。

【００３０】第1パスワード生成部123はICカード100の秘密キーと乱数貯蔵部122に貯蔵された乱数を読出し、所定の方法により一回用のパスワードを生成するブロックであって、図2に示したように対称キー暗号部200、ハッシュ関数部210、フォーマット変換部220により構成されている。

【００３１】対称キー暗号部200はICカード100の秘密キーと乱数貯蔵部122の乱数を読出して対称キー暗号アルゴリズムを使用して暗号を生成する。

【００３２】ハッシュ関数部210は対称キー暗号部200から生成された暗号を一方向ハッシュ(hash)関数に変換し、外部の不当な者が秘密キー及び乱数を逆追跡できなくする。

【００３３】フォーマット変換部220はハッシュ関数部210から出力されるパスワードビット列を使用者が読めるように所定のフォーマットに変換するブロックであって、パスワードビット列にカウンター貯蔵部127のカウンター値を挿入するカウンター挿入器222とカウンター挿入器222から出力されるパスワードビット列を使用者が読める所定のフォーマットに変換するフォーマット変換器224で構成される。

【００３４】カウンター挿入器222はまた少なくとも１つ以上の一回用のパスワード生成アルゴリズムのプロトコルを示すPTS(Protocol Type Selection)ビットを追加挿入することができる。

【００３５】フォーマット変換器224は望ましくは2進数よりなるパスワードビット列を使用者が読める10進数に変換する。

【００３６】第1乱数変更部124は第1パスワード生成部123から一回用のパスワードが生成されると乱数貯蔵部122に貯蔵された乱数値を所定の値に変更して乱数貯蔵部122に貯蔵する。

【００３７】表示部125は第1パスワード生成部123から生成されたパスワードをディスプレー(display)するブロックであって、望ましくはLCDが使われる。照会部126はICカード100の残額及び取引内訳を照会する。カウンター貯蔵部127は端末器120とサーバ140の同期を合せるためのカウンター値を貯蔵する。カウンター変更部128は一回用のパスワードを一回生成する度にカウンター値を所定の値に変更してカウンター貯蔵部127に貯蔵する。

【００３８】サーバ140は端末器120から生成された一回用のパスワードを認証するブロックであって、秘密キー貯蔵部141、第2パスワード生成部144、第2乱数変更部143、パスワード受信部142、パスワード検証部147、カウンター貯蔵部145、カウンター変更部146、カウンター抽出部148及び乱数同期部149よりなる。

【００３９】秘密キー貯蔵部141はICカード100に最初に貯蔵された秘密キー及び所定の乱数と同一な秘密キー及び乱数を貯蔵している。

【００４０】第2パスワード生成部144は秘密キー貯蔵部141に貯蔵された秘密キーと乱数を読出して端末器120で用いられる所定の方法と同一な方法により一回用のパスワードを生成するブロックであって、図3に示したように対称キー暗号部300、ハッシュ関数部310、フォーマット変換部320よりなる。対称キー暗号部300は秘密キー貯蔵部141に貯蔵された秘密キーと乱数を読出して秘密キー及び乱数を対称キー暗号アルゴリズムを使用して暗号を生成する。ハッシュ関数部310は対称キー暗号部300から生成された暗号を一方向ハッシュ(hash)関数に変換させて外部の不当な者が秘密キー及び乱数を逆追跡できなくする。フォーマット変換部320はハッシュ関数部310から出力されるパスワードビット列を所定のフォーマットに変換するブロックであって、パスワードビット列にカウンター貯蔵部145のカウンター値を挿入するカウンター挿入器322とカウンター挿入器322から出力されるパスワードビット列を使用者が読みやすく所定のフォーマットに変換するフォーマット変換器324で構成される。フォーマット変換器324は望ましくは2進数よりなるパスワードビット列を使用者が読みやすい10進数に変換する。

【００４１】第2乱数変更部143は第2パスワード生成部144から一回用のパスワードが生成されると秘密キー貯蔵部141の乱数値を端末器120の第1乱数変更部124と同一の乱数値に変更させて秘密キー貯蔵部141に貯蔵する。

【００４２】パスワード受信部142は端末器120の表示部125に示される一回用のパスワードを電話線や所定のネ

ットワークを通して受信する。パスワード検証部147は受信されたパスワードと生成されたパスワードが同一か否かを比較することにより一回用のパスワードを検証する。

【００４３】カウンター貯蔵部145は端末器120とサーバ140の同期を合せるためのカウンター値を貯蔵する。カウンター変更部146は一回用のパスワードを一回生成する度にカウンター値を所定の値に変更させてカウンター貯蔵部145に貯蔵する。カウンター抽出部148はパスワード受信部142により受信された一回用のパスワードからカウンター値を抽出し、端末器120のカウンター挿入器222からPTSが挿入されているとPTSを抽出する。

【００４４】乱数同期部149はカウンター抽出部148から抽出されたカウンター値とサーバ140のカウンター値が一致するか否かを比較して一致しない場合には、抽出されたカウンター値に相応する乱数を生成してサーバ140の対称キー暗号部300に入力させる。

【００４５】次いで、本発明による使用者認証装置及びその方法の動作を説明する。まず本発明を概略的に説明すれば次の通りである。本発明では既存の単純なパスワードを用いた認証の問題点を解決するために認証される度に使用するパスワードが変わる一回用のパスワードを使用する。一回用のパスワードを生成するための変数としては秘密キー、乱数及びカウンターを使用する。

【００４６】秘密キーは対称キー暗号アルゴリズムのためのものであって、暗号化のための秘密値として利用されて各使用者のICカード100に貯蔵される。

【００４７】乱数は毎回別のパスワードを生成させるためのものであって、毎回パスワードを変える乱数値であり、最初にはICカード100内にあるが、サービス初期化過程が行われる過程で端末器に伝達されて携帯用端末器120に保管され、ICカード内では削除される。

【００４８】カウンターは端末器120とサーバ140の同期を合せるためのものであって使用者の携帯用端末器120に保管される。乱数とカウンターは携帯用端末器120に貯蔵し、これらを用いて一回用のパスワードを生成する。そして使用者が多様な応用サーバから使用者認証を受けたいときは各サービス別のICカードと唯一つの端末器のみを有していれば良い。

【００４９】そして一回用のパスワードを生成する過程においてカウンター値をパスワードに含めて端末器120とサーバ140の同期を合わせることができる。サーバ140は先に使用者から受けたパスワードからカウンター値を抽出して同期を合せた後、端末器と既に共有していた秘密値と乱数値とを使用してパスワードを計算して使用者が送ったパスワードと一致するかを確認する。このようにカウンター値を利用すれば使用者の不注意によって端末器側のカウンターのみが変更されサーバ側のカウンターが変更されない場合にも端末器とサーバ間の同期を容易に合わせることができる。

【００５０】また、ICカード100は外部からカード内の秘密領域108に貯蔵された情報を読出すためにカード接近キーを提出するように要求する。カード接近キーを設定しておくことにより適法な使用者のみがカード内の秘密情報を読出すようにできるために使用者の秘密情報を安全に保管できる。

【００５１】本発明の動作をさらに詳しく説明する。まず本発明を機能別に分けると、残額及び取引内訳照会機能、一回用のパスワードの生成のためのサービス初期化機能、一回用のパスワード生成機能、そしてサーバにおいて一回用のパスワードの検証機能等がある。

【００５２】図4は本発明による使用者認証装置の使用者身分認証を行う全体的な動作を示す流れ図であって、本発明において一回用のパスワードを使用した使用者認証は大きく3段階で行われる。使用者がサービスを受けるために最初にICカードを端末器に挿入したときに行う初期化過程(470段階)、端末器内で一回用のパスワードを生成する過程(430段階)、そしてサーバで使用者のパスワードを検証する過程(450段階)である。

【００５３】まず、使用者は自分の希望する応用サービスのためのICカード100を端末器120のカード入力部121に挿入する(400段階)。使用者がICカードを挿入すれば端末器120のカード入力部121は各ICカードの種類を判別してICカード100が初めて挿入されたカードなのか、それとも既に一度挿入されて初期化が行われたカードなのかを検査する(410段階)。もし、初期化が必要なICカードの場合には初期化過程(470段階)を行う。一方、使用者が初期化の行われたICカードを挿入すれば、一回用のパスワードを生成するかを使用者が選択する(420段階)。普通の場合には残額照会(460段階)のみで終了し、仮りに使用者認証を希望する使用者は端末器の操作装置を用いて一回用のパスワードを生成することになる(430段階)。端末器120は初期化過程で受けたカード接近キーをICカード100に提出してカード内にある秘密値(対称キー暗号アルゴリズムのための秘密キー)を読出して一回用のパスワードを生成することになる(430段階)。使用者はこの結果をサーバ140に伝送すると(440段階)、サーバ140はこれを検証することになる(450段階)。

【００５４】図5はサービス初期化過程(470段階)をさらに詳しく示している。サービス初期化過程(470段階) は使用者がICカード100を最初に端末器120に挿入するときにICカードの公開領域に貯蔵された使用者認証に必要な重要情報である乱数と使用者のICカードの秘密領域に貯蔵された秘密キーとを読出すためのカード接近キーを端末器に伝達して公開領域で乱数とカード接近キーとを削除する過程である。使用者がICカード100を端末器120に最初に挿入すれば(図4の400段階)、端末器120はICカード100が最初に挿入されたことを認識して初期化過程を行う。端末器120はICカード100の公開領域に貯蔵された乱数とカード接近キーとを読出し(510段階)、端末器120

の乱数貯蔵部122に貯蔵した後(520段階)、ICカード100の公開領域に貯蔵された乱数とカード接近キーとをICカード100から削除する(530段階)。従って、使用者が初期化過程を終えたICカードには秘密キーのみが安全な秘密領域に残ることになる。

【００５５】そして、残額照会のためのICカードの情報は誰でも読出できるようになっており、使用者認証のための秘密キーは秘密領域に貯蔵されており、この値を読出すためにはカード接近キーが必要である。サービス初期化過程が行われるとICカード内の秘密キーは唯初期化過程を行った端末器のみ読出できることになる。使用者は１つの端末器で多様なサービスのための一回用のパスワードを発生させうる。端末器内では各サービスのために別の記憶場所を割り当てて各サービスの使用者認証に必要な情報を保管している。

【００５６】図6は図4の一回用のパスワード生成段階(430段階) のさらに詳しい動作を示す流れ図であって、一回用のパスワードはICカード100とサーバ140が共有している秘密キー(対称キー暗号アルゴリズムのための秘密キー等)と端末器120とサーバ140が共有している乱数値で生成する。使用者がICカードを端末器に挿入し(図4の400段階)、一回用のパスワードを生成するための端末器の操作装置を操作すれば端末器120内の第1パスワード生成部123の対称キー暗号部200はICカード100から秘密キーを読出し、乱数貯蔵部122から乱数とカウンター値を読出し(610段階)、これらによって対称キー暗号アルゴリズムを使用して暗号を生成する(620段階)。それからハッシュ関数部210により一方向ハッシュ(hash)関数を使用して２進数の結果値を計算する(630段階)。この一方向ハッシュ関数を使用することは攻撃者が一回用のパスワードの結果を用いて秘密値に対する何れの情報も分からなくするためのものである。

【００５７】一方向ハッシュ関数の結果値は一回用のパスワードで直ちに使用出来ないために変換アルゴリズム過程を経る(680段階)。まず、２進数の結果では使用者は慣れていないために使用者が容易に利用しうる十進数に変換する。変換アルゴリズムを利用して２進数の結果値を十進数に変えた一回用のパスワードを画面表示部125に示す(690段階)。２進数で出力される一方向ハッシュ関数の結果が非常に大きな数なので(例えば２進数で64ビット以上の数)端末器の表示部125に示しうる範囲(例えば、一回用のパスワードとして8桁の十進数を使用する場合に２進数で26ビットの数程度)にすべきである。

【００５８】変換アルゴリズム(680段階)では一方向ハッシュ関数の結果値とカウンター値、PTS(Protocol Type Selection)が使われる。ここでPTS(Protocol Type Selection)とカウンター値Nは使用者の端末器120とサーバ140の間の同期を合せるためにカウンター挿入器222により一回用のパスワードのビット列内に挿入される。例えば26ビットのパスワード中には一方向ハッシュ関数の結果値が占める領域とカウンター値Nと、PTSが占める領域に区分されており、この全体値が１つの一回用のパスワードとなる。PTSは一回用のパスワードを生成するアルゴリズムが多様になるときサーバ側からこれを区分するためのものである。

【００５９】カウンター値Nは一定の大きさの数字から始めてパスワードを一度生成する度に1ずつ減少するが(650段階)、この値が0であるかを検査し(640段階)、0となると再び初期化をすることになる(660段階)。乱数も同様に普通は1ずつ増加させるが、Nが0になると初期化させる。サービス初期化の過程において初期化用のICカードから読出して使用した乱数は最初のパスワード発生時にのみ使用し、それ以降には乱数を1ずつ増加させて使用する(650段階)。カウンター値Nが0となったときにはパスワード生成中に発生した乱数(例えば、対称キー暗号アルゴリズムの結果値)を乱数初期値として設定する。この乱数を再び1ずつ増加させながらパスワードを生成し(650段階)、カウンター値Nが0になると新たな乱数を設定することになる(660段階)。一回用のパスワードを生成した後、カウンターNと乱数RNは端末器の乱数貯蔵部122に記録される(670段階)。

【００６０】図7はサービス提供者のサーバ140において使用者が伝送したパスワードを検証する過程を示した流れ図である。サーバ140は使用者が伝送した一回用のパスワードをパスワード受信部142を通して受信する(700段階)。それからカウンター抽出部148により受信されたデータビット列からカウンター値を抽出し(710段階)、端末器120と同期を合せる。一方サーバ140は同期の合わせられた乱数と秘密値であって端末器と同じ方法で一回用のパスワードを生成する(720段階)。一回用のパスワードを生成する過程は端末器と同一なのでここでは説明を略す。次いで、生成された一回用のパスワードを使用者のものと比較し(730段階)、パスワードが一致すると使用者の身分を認証することになる(770段階)。

【００６１】使用者が伝送したパスワードがサーバ140から発生したパスワードと一致しないのは不法使用者の攻撃や使用者の端末器120とサーバ140との同期が合わないためである。適法な使用者が伝送した一回用のパスワードが合わない場合は使用者の不注意や故意により端末器120のカウンターとサーバ140とのカウンター値が合わない場合である。即ち、受信した端末器120のカウンター値とサーバ140のカウンター値とが同一であっても、カウンターの周期N自体が間違っていることによる乱数値の相異によってパスワードが一致しない場合が発生しうる。サーバ140はこれを補償するためにカウンターの周期単位でカウンター値と乱数を増加させてパスワードを計算して比較することになる。サーバ140は周期N番の以降のパスワードを計算するためにN番のパスワードを全て計算する必要はない。ただし、Nが0となったとき、新たな乱数を設定するための計算のみが追加して必要に

なるのでサーバの計算量には大きな負担はない(760段階)。N番以降のパスワードも一致しない場合には再びN番以後のパスワードを計算して比較することになるが、このような過程を必要に応じて何回まで反復するかを設定できる(740段階)。もし、指定された範囲内でパスワードが一致しないとこれは攻撃者の攻撃と判断してサービスを拒絶することになる(750段階)。

【００６２】前述したように使用者のICカード100と携帯用端末器120のみを利用する使用者の認証に付け加えて使用者が記憶しているパスワードを使用して保安水準をさらに向上させることもできる。もし、使用者がICカード100と端末器120とを全てなくした後、その持主に対する個人情報を知っている他人が習得して使用者認証を受けることができる。本認証システムの使用者認証過程に追加で各使用者のみが記憶しているパスワードを確認する過程を追加するとさらに安全な使用者認証が可能である。即ち、使用者が適法な使用者だと身分認証を受けるためには自分のみが記憶しているパスワード、自分のみのICカードと一回用のパスワードを生成する携帯用端末器を有するべきである。

【００６３】一方、前述したように使用者は一回用のパスワードを発生させるために端末器を使用し、端末器には使用者毎に他の一回用のパスワードを発生させるための固有の秘密キーがある。そして、この秘密キーは使用者が伝送した一回用のパスワードを検証するためにサーバにおいても有するべきである。この際、秘密キーは端末器を製造する工場で端末器に挿入できる。しかし、サービス提供者が生産された端末器に対して使用者登録をする際、秘密キーを端末器に挿入することが望ましい。そして、サービス提供者は端末器のための秘密キーを生成し、これをICカードを通して端末器に挿入すると同時にこれをサーバに登録する。

【００６４】これにより、製造工場で端末器を生産するときは秘密キー挿入に対する別の手順が不要となり、工場での端末器の大量生産時に生産性を向上させうる。また、使用者認証のための秘密キーはサービス提供者のみが知っているために露出される危険がないため安全であり、端末器生産者やサービス提供者は端末器が使用者に供給される前に特別な管理をする必要がない。

【００６５】

【発明の効果】本発明では既存の単純なパスワードを用いた認証の問題点を解決するために認証を受ける度に使用するパスワードが変わる一回用のパスワードを使用することにより保安水準を高めた。

【００６６】そして本発明では身分の認証のために使用者が有しているICカード100と使用者が有する端末器120とが一致してからこそ正確な一回用のパスワードが生成され、身分認証を通過させることにより、もし他人の端末器やICカードを習得したとしても決して正しいパスワードを生成できないので既存の使用者認証方式に比べて保安水準が高まる。またさらに安全な使用者認証のための身分認証過程で使用者のみが記憶しているパスワードを確認する過程を追加することにより、使用者は身分認証を受けるためには自分のみが知っているパスワード、使用者のICカードと一回用のパスワード生成端末器の３つが必ず一致して初めて適法な使用者として認証される。

【００６７】また、本発明では使用者が一回用のパスワードを発生するために、使用者の秘密情報を記憶しているICカードはカード内の情報を読出すためのカード接近キーを設定することにより、秘密情報の露出が防げ、使用者は１つの端末器で多様なサービスのための一回用のパスワードを発生できるために非常に経済的である。

【００６８】また、本発明では一回用のパスワードを生成するために乱数を使用し、使用者の端末器とサービス提供者のサーバの同期を合せるためにカウンターを使用することにより、既存のサービスにおいて使用者認証のためのシステムにソフトウェア的に実現しやすくした。これによりサービス提供者に追加負担を与えなく経済的に使用者認証を強化しうる。

【００６９】本発明における使用者認証装置及び方法は使用者認証が必要な全ての所に適用しうる。銀行のテレバンキング、PCを用いたホームショッピングとホームバンキング、有料PC通信、ネットワークサービス等の安全な使用者認証が必要な全ての所に使用しうる。特にサービスを受けるために使用者はサービス登録のため直接サービス提供者を尋ねなくても良い長所がある。使用者がサービスを申込んだ後、サービス提供者からICカードを郵便で提供され、端末器は市販品を容易に購入した後、安全な使用者認証サービスが受けられる。これは使用者が直接サービス提供者を尋ねにくい状況で非常に便利である。またサービス提供者の立場では大量普及されるサービスに対して一般使用者と直接対しなくても良いので業務上の負担を大幅に軽減しうる。

【００７０】本発明で使用される端末器は一回用のパスワードの生成だけでなく一般のICカードの電子貨幣のための残額及び取引内訳照会機能を有している。今後、電子貨幣の普及が加速化されることを予想する際、１つの端末器で非常に有用に使用しうる。

【図面の簡単な説明】

【図１】本発明による使用者認証装置の構成を示したブロック図である。

【図２】第1パスワード生成部の詳細な構成を示したブロック図である。

【図３】第2パスワード生成部の詳細な構成を示したブロック図である。

【図４】本発明による使用者認証装置の使用者身分認証を行う全体的な動作を示した流れ図である。

【図５】サービス初期化過程をさらに詳しく示した流れ図である。

19　　20

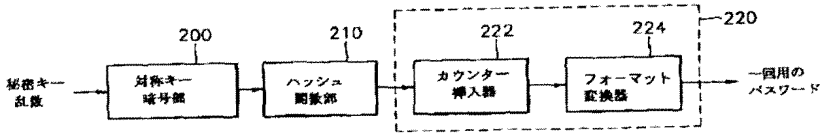
【図６】図4の一回用のパスワード生成段階のさらに詳細な動作を示した流れ図である。

【図７】サービス提供者のサーバで使用者が伝送したパスワードを検証する過程を示した流れ図である。

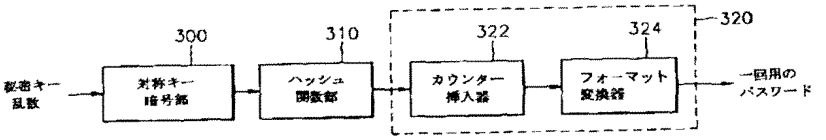
【符号の説明】

１、８　アドレスレコーダ
２、３、９　ＲＯＭ
４、６、１１　マックス
５、７、１２　Ｄフリップフロップ
１０　遅延部
２１　輪郭色差信号設定部
＊２２　形状色差信号設定部
２３　スレショルド色差信号設定部
２４　位置信号発生部
２５　色差信号選択部
４１　輝度信号遅延部
４２　重畳輝度信号設定部
４３　輪郭輝度信号設定部
４４　スレショルド輝度信号設定部
４５　位置信号発生部
４６　輝度信号選択部

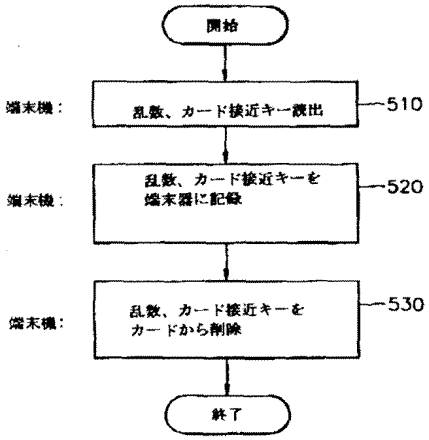
【図２】



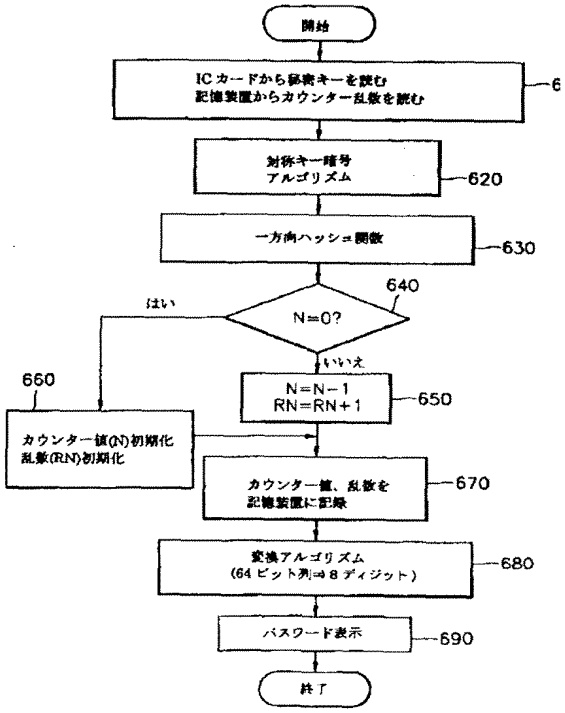
【図３】



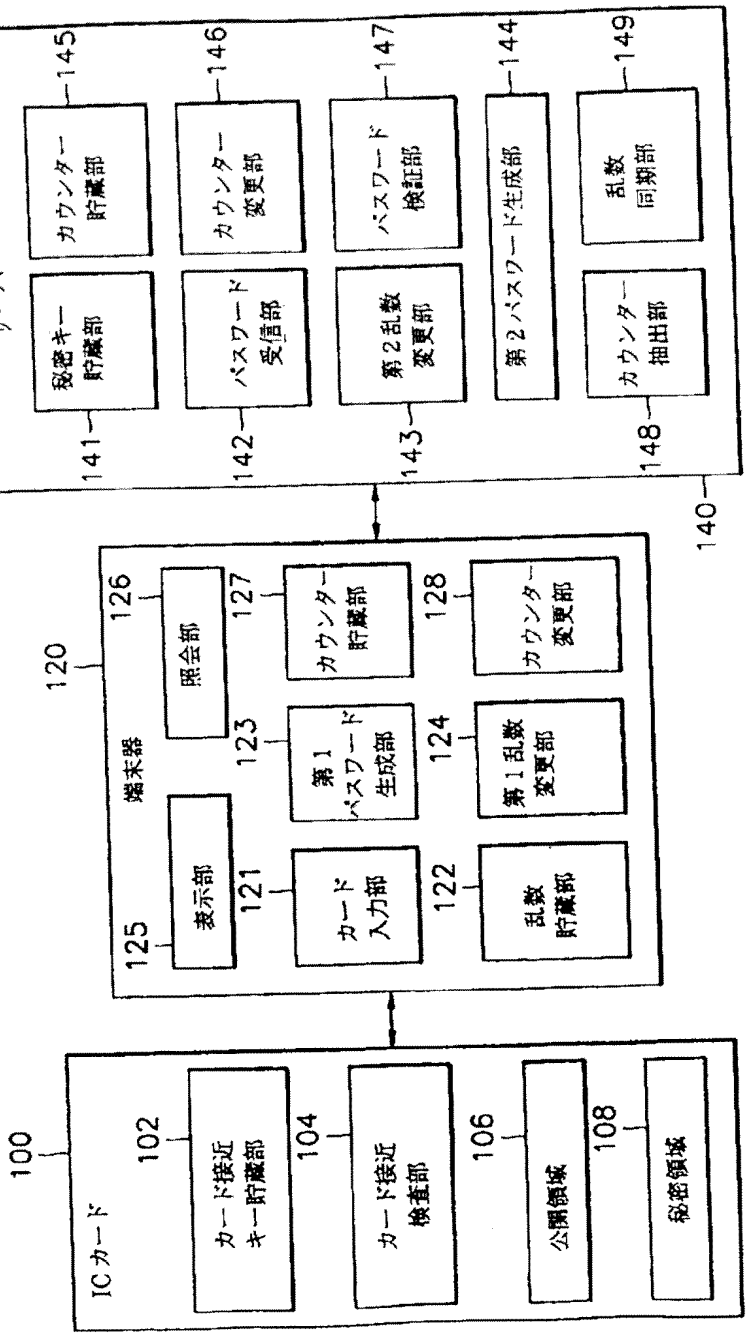
【図５】



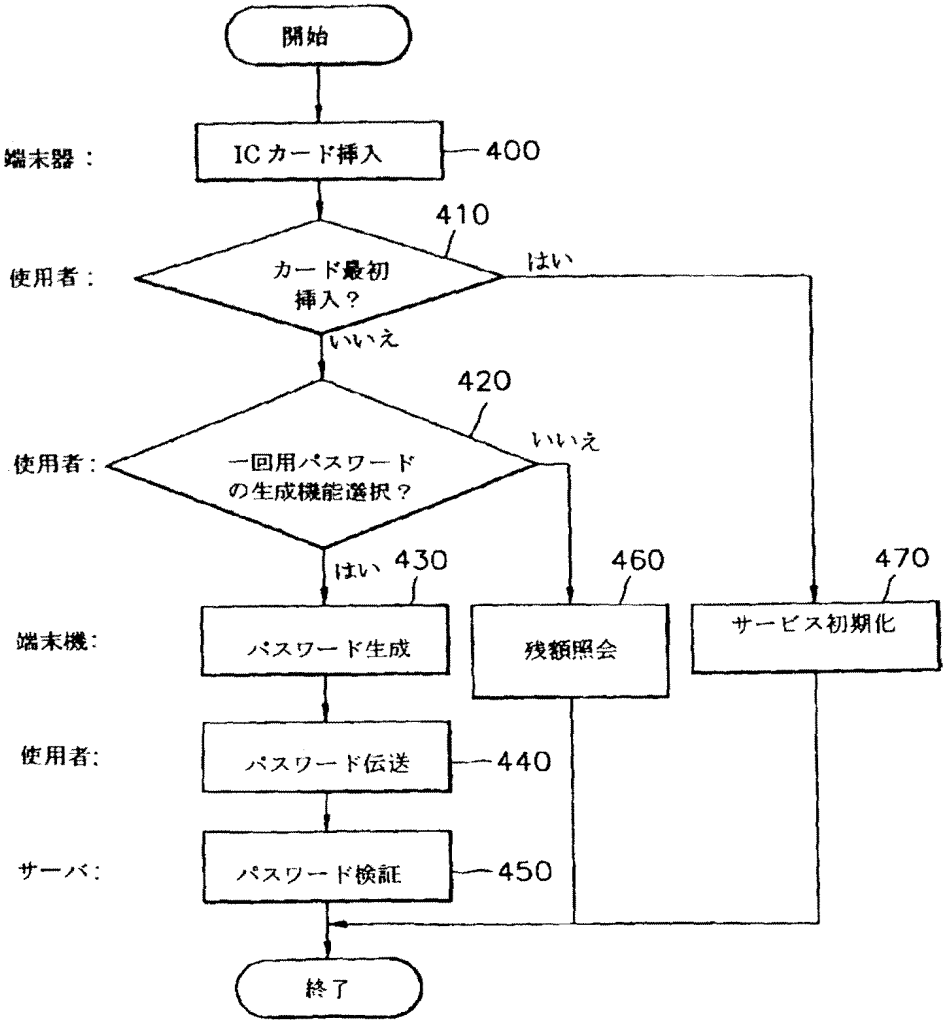
【図６】



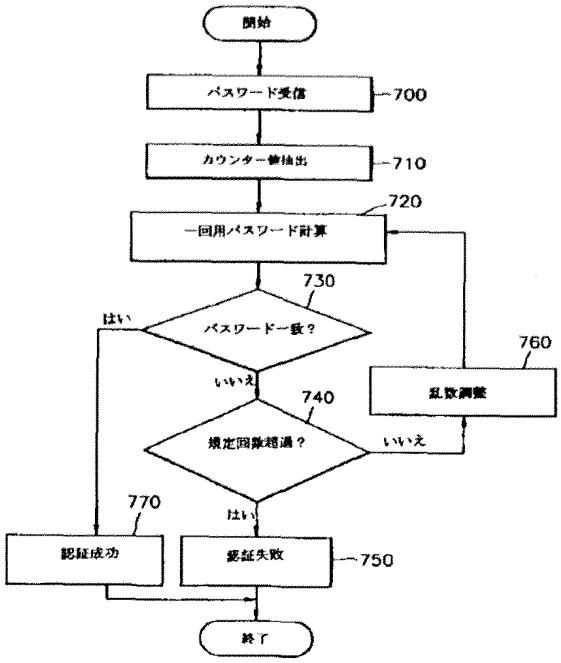
【図１】


サーバ
秘密キー貯蔵部
141
カウンター貯蔵部
145
パスワード受信部
142
カウンター変更部
146
第２乱数変更部
143
パスワード検証部
147
第２パスワード生成部
144
カウンター抽出部
148
乱数同期部
149
140
端末器
120
表示部
125
照会部
126
カード入力部
121
第１パスワード生成部
123
乱数貯蔵部
122
第１乱数変更部
124
カウンター貯蔵部
127
カウンター変更部
128
ICカード
100
カード接近キー貯蔵部
102
カード接近検査部
104
公開領域
106
秘密領域
108

【図４】


開始
端末器：
ICカード挿入
400
410
使用者：
カード最初
挿入？
はい
いいえ
420
使用者：
一回用パスワード
の生成機能選択？
いいえ
はい
430
460
470
端末機：
パスワード生成
残額照会
サービス初期化
使用者：
パスワード伝送
440
サーバ：
パスワード検証
450
終了

【図７】



フロントページの続き

(51)Int.Cl.[5]	識別記号	ＦＩ	
		Ｈ０４Ｌ　9/00	６７３Ｅ
			６７３Ｃ